PATENT **MS150832.02/MSFTP150US**

CERTIFICATE OF FACSIMILE TRANSMISSION
I hereby certify that this correspondence (along with any paper referred to as being attached or enclosed) is being faxed to 571-273-8300 on the date shown below to Mail Stop Appeal Brief - Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Date: 8-8-05

Himanshu S. Amin

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re patent application of:			
Applicant(s):	Michael Ginsberg	Examiner:	Syed Zia
Serial No:	09/671,388	Art Unit:	2131
Filing Date:	September 27, 2000		

Title: TRUST LEVEL BASED PLATFORM ACCESS REGULATION APPLICATION

08/09/2005 MBINAS 00000035 09671388
01 FC:1402 500.00 OP

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF

Dear Sir:

Applicant's representative submits this brief in connection with an appeal of the above-identified patent application. A credit card payment form is filed concurrently herewith in connection with all fees due regarding this appeal brief. In the event any additional fees may be due and/or are not covered by the credit card, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1063 [MSFTP150US].

I. Real Party in Interest (37 C.F.R. §41.37(c)(1)(i))

The real party in interest in the present appeal is Microsoft Corporation, the assignee of the present application.

II. Related Appeals and Interferences (37 C.F.R. §41.37(c)(1)(ii))

Appellant, appellant's legal representative, and/or the assignee of the present application are not aware of any appeals or interferences which may be related to, will directly affect, or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. Status of Claims (37 C.F.R. §41.37(c)(1)(iii))

Claims 1-5 and 7-20 are currently pending in the subject application and are presently under consideration. Claims 1-5 and 7-20 stand rejected by the Examiner, and claim 6 has been cancelled. The rejection of claims 1-5 and 7-20 is being appealed.

IV. Status of Amendments (37 C.F.R. §41.37(c)(1)(iv))

No amendments have been entered subsequent the Final Office Action dated March 7, 2005.

V. Summary of Claimed Subject Matter (37 C.F.R. §41.37(c)(1)(v))

A. Independent Claim 1

Independent claim 1 recites a system that regulates access to a distributed computing platform that comprises a component that analyzes an application that requests access to the distributed computing platform, the component determines a level of access to the distributed computing platform and applies a trust level to the application corresponding to the determined level of access; and a component that compares the applied trust level of the application with a trust level of a module called by the application and regulates access of the application to the distributed computing platform based at least in part upon the comparison. (*See e.g.*, page 2, lines 9-22).

B. Independent Claim 10

Independent claim 10 recites a system for regulating access to a distributed computing platform that comprises means for determining a trust level for an application, the application requesting access to the distributed computing platform (*See, e.g.*, page 4, lines 24-27), means for applying the trust level to the application to regulate access to the distributed computing platform (*See, e.g.*, page 7, lines 11-15), and means for regulating access of the application to the distributed computing platform by analyzing a trust level of a module called by the application (*See, e.g.*, page 4, lines 17-23).

The "means for" limitations described above are identified as limitations subject to the provisions of 35 U.S.C. §112 ¶6. The structures corresponding to these limitations are identified with reference to the specification and drawings in the above noted parentheticals.

C. Independent Claim 12

Independent claim 12 recites a method for regulating access to a distributed computing platform that comprises determining a trust level for a first module called by an application, the application requesting access to the distributed computing platform, and regulating access of the application to the distributed computing platform based at least in part upon the determined level of trust for the first module. (*See, e.g.*, page 8, line 27 – page 9, line 10).

VI. Grounds of Rejection to be Reviewed (37 C.F.R. §41.37(c)(1)(vi))

A. Claims 1-5 and 7-20 stand rejected under 35 U.S.C. §102(e) as being anticipated by Anglin (US 6,260,069).

VII. Argument (37 C.F.R. §41.37(c)(1)(vii))

A. Rejection of Claims 1-5 and 7-20 Under 35 U.S.C. §102(e)

Claims 1-5 and 7-20 stand rejected under 35 U.S.C. §102(e) as being anticipated by Anglin (US 6,260,069). Reversal of this rejection is respectfully requested for at least the following reason. Anglin does not disclose each and every element of appellant's invention as claimed.

> For a prior art reference to anticipate, 35 U.S.C. §102 requires that "each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *In re Robertson*, 169 F.3d 743, 745, 49 USPQ2d 1949, 1950 (Fed. Cir. 1999) (*quoting Verdegaal Bros., Inc. v. Union Oil Co.*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987)).

The subject invention facilitates regulating access to a distributed computing platform with respect to untrusted and/or partially trusted applications/modules. To that end, independent claim 1 recites a component that ***compares an applied trust level of an application with a trust level of a module called by the application and regulates access of the application to a distributed computing platform based at least in part upon the comparison***. Similarly, independent claim 10 recites ***means for regulating access of an application to a distributed computing platform by analyzing a trust level of a module called by the application***, and independent claim 12 recites ***determining a trust level for a first module called by an application, the application requesting access to the distributed computing platform, and regulating access of the application to the distributed computing platform based at least in part upon the determined level of trust for the first module***. Anglin does not disclose or suggest these aspects of appellant's invention.

In contrast to the claimed invention, Anglin discloses a system utilized for backing up files in a distributed computing system, wherein a backup program is initiated to request backup of a particular file. As described by the Examiner in the Final Office Action dated March 7, 2005, and again in the Advisory Action dated May 3, 2005, to

effectuate backing up a file, a determination is made regarding whether the file exists within a shared namespace. If it is found that the file is resident within the shared namespace, a backup request is transmitted to a backup server program, and such program transmits a message to a file server to provide the requested file. The backup server program subsequently stores the requested file in a storage device. The Examiner asserts that due to the above, Anglin "describes and provides an access regulation system that can analyze and interact with a computing environment." Yet, the description of Anglin provided by the Examiner does not even tangentially relate to an access regulation system, much less the above-referenced claim aspects. More specifically, the Examiner emphasizes that a backup request is transmitted by a client program *upon determining that* a requested file is maintained in a shared namespace. Again, this determination does not relate to access regulation, but rather refers to determining whether a file that is desirably subject to backup is existent within a shared namespace.

Anglin does, however, disclose a form of access regulation with respect to client devices. In more detail, Anglin teaches that a user logs into a client to gain access to a distributed computing environment as well as files maintained in a shared namespace managed by a file server. (*See* col. 4, lines 1-3, col. 5, lines 19-22). An authentication service can then grant the client an authentication ticket that describes a level of access allowed for the client with respect to files within the file server. (*See* col. 5, lines 22-26). Anglin further discloses that the authentication ticket provides access to services and files throughout the distributed computing environment, including files within the file server. (*See* col. 4, lines 3-8, col. 5, lines 33-35). Thus, in summary, Anglin generally teaches determining whether a client has access to a distributed computing environment, and specifically teaches determining whether a client has access to files within a file server (that can be subject to backup). The authentication ticket, however, is not applied to ***an application,*** and there is no ***comparison of an applied trust level of an application with a trust level of a module called by the application***.

The cited reference discloses determining whether a device has access to a distributed computing environment without regard to any sort of ***comparison***. In more detail, the claimed invention enables a fully trusted application to call and utilize a partially trusted module (in a read-only manner) by comparing the trust levels associated

with the application and the module, while Anglin teaches providing an authentication ticket to a client machine (associated with a user) based upon a user name and password. In still more detail, the access ticket provides a client with access to files, which are not associated with any sort of trust level. Thus, even if the granted access were equated to a ***trust level*** as claimed, there is no disclosure within Anglin of any module, file, or other computer component being associated with a trust level, and thus no ***comparison*** between a trust level assigned to the client and a trust level assigned to a disparate component can be undertaken. In other words, it is readily apparent that the claimed invention recites *two* disparate trust levels: ***an applied trust level of an application*** and ***a trust level of a module called by the application.*** (*See, e.g.*, claims 1, 10, and 20). Anglin, at most, discloses a single trust level – one applied (by way of an access ticket) to a client that is attempting to access files within a file server. Accordingly, per the teachings of Anglin, as there is (at most) one trust level applied to a client, there cannot be a ***comparison*** of trust levels (as a comparison requires at least two entities).

Furthermore, there is no disclosure within Anglin of a ***module called by the application*** – rather, a user initiates the backup request by communicating with the client. Accordingly, Anglin fails to disclose ***determining a trust level for a first module called by an application, the application requesting access to the distributed computing platform*** as recited in independent claim 12. To be more explicit, Anglin discloses determining whether a client is authorized to access a file – but the client is not ***called by an application*** as claimed.

Referring now to dependent claims 3 and 13, it is apparent from the above that Anglin further does not disclose or suggest (inherently or otherwise) ***marking the application with at least one of states: (1) fully trusted, (2) run restricted, and (3) fail to load*** as recited in these claims. In particular, Anglin at most discloses applying a binary trust level to a *client* upon receipt and analysis of an access ticket provided by user, and not to an ***application*** as claimed. The Examiner has stated that the above element "can be implemented by a person of ordinary skill in the art..." Such a conclusory phrase, however, is not representative of the Examiner's burden under 35 U.S.C. §102.

> Inherency, however, may not be established by probabilities or possibilities. The mere fact that a certain thing may result from a given set of circumstances is not sufficient." *Mehl/Biophile Int'l Corp. v. Milgraum*, 192 F.3d 1362, 1365, 52 USPQ2d 1303, 1305 (Fed. Cir. 1999), reh'g denied, 1999 U.S. App. LEXIS 31386 (Fed. Cir. Oct. 27, 1999) (*quoting In re Oelrich*, 666 F.2d 578, 581, 212 USPQ 323, 326 (CCPA 1981)).

Moreover, Anglin does not provide any motivation for utilizing levels of trust (*e.g., **(1) fully trusted, (2) run restricted, and (3) fail to load***). As described above, Anglin relates to a system utilized for backing up files in a distributed computing system, and does not relate to applications that are associated with trust levels. In particular, the security described within Anglin is binary, wherein a client either has authority to access a file for backup or does not have authority to access a file for backup. Accordingly, Anglin does not disclose, teach, or suggest the limitations of claims 3 and 13.

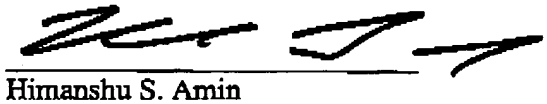
In view of the foregoing, it is submitted that Anglin does not anticipate nor make obvious the invention as recited in claims 1, 10, and 12 (and claims 2-5, 7-9, 11, and 13-20 which respectfully depend there from). Accordingly, this rejection should be reversed.

B. Conclusion

For at least the above reasons, the claims currently under consideration are believed to be patentable over the cited references. Accordingly, it is respectfully requested that the rejections of claims 1-5 and 7-20 be reversed.

If any additional fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP150US].

Respectfully submitted,
AMIN & TUROCY, LLP



Himanshu S. Amin
Reg. No. 40,894

AMIN & TUROCY, LLP
24th Floor, National City Center
1900 East 9th Street
Telephone: (216) 696-8730
Facsimile: (216) 696-8731

VIII. Claims Appendix (37 C.F.R. §41.37(c)(1)(viii))

1. A system that regulates access to a distributed computing platform comprising:

a component that analyzes an application that requests access to the distributed computing platform, the component determines a level of access to the distributed computing platform and applies a trust level to the application corresponding to the determined level of access; and

a component that compares the applied trust level of the application with a trust level of a module called by the application and regulates access of the application to the distributed computing platform based at least in part upon the comparison.

2. The system of claim 1, the component that analyzes the application providing for inheritance of the trust level.

3. The system of claim 1, the component that analyzes the application providing for marking the application with at least one of states: (1) fully trusted, (2) run restricted, and (3) fail to load.

4. The system of claim 1, wherein the component is stored in a Read Only Memory (ROM) in the platform.

5. The system of claim 1, wherein the component is part of an operating system.

6. (Cancelled).

7. The system of claim 1, wherein the functionality of one or more Application Programming Interface (API) calls, when called by the application, are selectively restricted.

8. The system of claim 7, wherein selectively restricting the functionality of the one or more API calls includes restricting the functionality to read functions.

9. The system of claim 8, wherein selectively restricting the functionality of the one or more API calls includes terminating the application.

10. A system for regulating access to a distributed computing platform, comprising:

means for determining a trust level for an application, the application requesting access to the distributed computing platform;

means for applying the trust level to the application to regulate access to the distributed computing platform; and

means for regulating access of the application to the distributed computing platform by analyzing a trust level of a module called by the application.

11. The system of claim 10 further comprising means for applying the trust level to one or more modules called by the application.

12. A method for regulating access to a distributed computing platform, comprising the steps of:

determining a trust level for a first module called by an application, the application requesting access to the distributed computing platform; and

regulating access of the application to the distributed computing platform based at least in part upon the determined level of trust for the first module.

13. The method of claim 12 wherein determining the trust level for the first module further comprises the step of marking the first module with at least one of states: (1) fully trusted, (2) run restricted, and (3) fail to load.

14. The method of claim 12 wherein determining the trust level for the first module further comprises transmitting the first module to a verification program.

15. The method of claim 12 wherein regulating access to the distributed computing platform further comprises selectively aborting calls made to one or more APIs.

16. The method of claim 12 wherein regulating access to the distributed computing platform further comprises selectively terminating the first module.

17. The method of claim 12 wherein a program for determining the trust level for the first module is stored in a ROM in the platform.

18. The method of claim 12 wherein the logic for applying the trust level to regulate access to the platform is stored in a ROM in the platform.

19. The method of claim 12 wherein the trust level may be inherited.

20. The method of claim 12 wherein the trust level may be applied to one or more second modules called by the first module.

IX. Evidence Appendix (37 C.F.R. §41.37(c)(1)(ix))

None.

X. Related Proceedings Appendix (37 C.F.R. §41.37(c)(1)(x))

None.